REMARKS

Claims 19-40 are now pending in the application. Claims 37 and 40 are currently amended. No new matter has been added as all amendments are supported by the specification, claims and drawings as originally filed. The Examiner is respectfully requested to reconsider and withdraw the rejection(s) in view of the amendments and remarks contained herein.

CLAIM OBJECTIONS

Claim 40 is objected to because of certain informalities. Applicant has amended claim 40 to address this objection according to the Examiner's suggestions. Therefore, reconsideration and withdrawal of this objection are respectfully requested.

REJECTION UNDER 35 U.S.C. § 103

Claims 37-40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Asano (U.S. Pat. No. 7,088,822). This rejection is respectfully traversed.

Applicant has amended claim 37, which now recites "the multiple first sub-secret-keys are divided into k groups" and "equation combination representation including t items of j and i, j is sequence number of the group which has the first sub-secret-keys, and i is number of the first sub-secret-key in the j^{th} group, each of j in one equation combination representation is different, j, i, k, and t are positive integers, and t is less than k".

Applicant submits that Asano is not a prior art to the subject application. The subject application claims the benefit of the Chinese application 01136018.6, filed on September 28, 2001. The effective filing date of Asano is February 13, 2002.

Assuming arguendo that Asano is a prior art, Applicant submits that Asano fails to teach or suggest the above mentioned limitations. Claim 37 is directed to issuance of a digital certificate. Asano at best appears to disclose updating the node key. See, column 21, lines 25-50, FIGs 11 and 12A.

Asano at best appears to disclose that the devices 0, 1, and 2 can obtain the updated K(R) by multiple decryption calculations. See, column 21, lines 25-50, Figs. 11 and 12A. The device 2 obtains the K(t)001 by using its leaf key K0010 to decrypt encryption key Enc(K0010, K(t)001). Similarly, the results of the decryption calculations, i.e., the K(t)00, K(t)0, are obtained based on the encryption key Enc of child node and K(t) of the adjacent leaf node. In this example, the updated K(R) can be obtained by the calculations according to the encryption keys and the leaf key K0010.

Systems embodying the claimed invention can have the following advantages. The corresponding relationship between the first sub-secret-keys and the second sub-secret-keys is expressed by the equation combination representation, and the equation combination representation is not a function for calculation. Therefore the processes of issuing digital certificate can be simplified. Moreover, the equation combination representation includes some items of sequence number of group and number of the first sub-secret-key in the group, and each sequence number of group in the equation combination representation is different, so the equation combination representation

does not include the first sub-secret-keys, which protects the first sub-secret-keys from being leaked.

Claims 37-40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Asano and further in view of Yung (US 2002/0076052). This rejection is respectfully traversed.

Yung at best appears to disclose an RSA function for secure systems is used, the private key is a sum of sub-secret-keys, and the digital signature is generated by using modular multiplication. See, paragraph 43, and 63-66. Thus, Asano and Yung, individually or in combination, fail to teach or suggest above-mentioned limitations of claim 37.

Applicant submits herewith an English translation of the priority document of the present invention. The English translation of the priority document supports the claims of the subject patent application. Applicant will submit a statement that the translation is accurate in due course.

In view of the foregoing, Applicant submits that claim 37 and its dependent claims 38-40 define over the art cited by the Examiner.

ALLOWABLE SUBJECT MATTER

Applicant thanks the Examiner and acknowledges that claims 19-36 are allowed.

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action and the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 08-0750, under Order No. 9896-000013/US from which the undersigned is authorized to draw.

Dated: January 17, 2008

Respectfully submitted,

By /Joseph M. Lafata/
Joseph M. Lafata
Registration No.: 37,166
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1223
Attorney for Applicant